Las copias de seguridad cifradas de bóvedas robadas durante la filtración de datos de LastPass en 2022 han permitido que actores maliciosos aprovechen contraseñas maestras débiles para descifrarlas y vaciar activos en criptomonedas incluso hasta finales de 2025, de acuerdo con nuevos hallazgos de TRM Labs.

La empresa de inteligencia blockchain señaló que las evidencias apuntan a la participación de ciberdelincuentes rusos en estas actividades, destacando que uno de los intercambios rusos recibió fondos vinculados a LastPass tan recientemente como en octubre.

Esta evaluación se basa *"en el conjunto total de evidencias en la cadena, que incluyen interacciones repetidas con infraestructura asociada a Rusia, continuidad en el control antes y después de las operaciones de mezcla, y el uso constante de intercambios rusos de alto riesgo como vías de salida"*, agregó la compañía.

En 2022, LastPass fue víctima de un ataque significativo que permitió a los atacantes acceder a información personal de sus clientes, incluidas las bóvedas de contraseñas cifradas que contenían credenciales sensibles, como claves privadas de criptomonedas y frases semilla.

A principios de este mes, el servicio de gestión de contraseñas fue multado con 1.6 millones de dólares por la Oficina del Comisionado de Información del Reino Unido (ICO), debido a la falta de medidas técnicas y de seguridad suficientemente sólidas para evitar el incidente.

La brecha también llevó a la empresa a emitir una advertencia en su momento, indicando que los actores maliciosos podrían emplear técnicas de fuerza bruta para adivinar las contraseñas maestras y descifrar los datos robados. Los hallazgos más recientes de TRM Labs confirman que los ciberdelincuentes llevaron a cabo exactamente ese escenario.

"Cualquier bóveda protegida por una contraseña maestra débil podría eventualmente ser descifrada sin conexión, convirtiendo una sola intrusión en 2022 en una ventana de varios años para que los atacantes rompan contraseñas de forma silenciosa y drenen activos con el paso del tiempo", indicó la empresa.

"A medida que los usuarios no rotaron sus contraseñas ni reforzaron la seguridad de sus bóvedas, los atacantes continuaron descifrando contraseñas maestras débiles años después, lo que derivó en vaciamientos de billeteras incluso a finales de 2025".

Los vínculos rusos con las criptomonedas robadas durante la filtración de LastPass de 2022 se explican principalmente por dos factores: el uso de intercambios comúnmente asociados con el ecosistema de ciberdelito ruso dentro del proceso de lavado y las conexiones operativas identificadas a partir de billeteras que interactuaron con mezcladores antes y después de las etapas de mezcla y blanqueo.

Se han rastreado más de 35 millones de dólares en activos digitales sustraídos, de los cuales 28 millones fueron convertidos a Bitcoin y lavados mediante Wasabi Wallet entre finales de 2024 y comienzos de 2025. Otros 7 millones de dólares se vincularon a una segunda ola detectada en septiembre de 2025.

Se determinó que los fondos robados fueron canalizados a través de Cryptomixer.io y posteriormente retirados mediante Cryptex y Audia6, dos intercambios rusos relacionados con actividades ilícitas. Cabe señalar que Cryptex fue sancionado por el Departamento del Tesoro de Estados Unidos en septiembre de 2024 por haber recibido más de 51.2 millones de dólares en fondos ilícitos provenientes de ataques de ransomware.

TRM Labs indicó que logró desanonimizar estas operaciones a pesar del uso de técnicas CoinJoin, diseñadas para dificultar el rastreo de fondos, al identificar retiros agrupados y cadenas de "pelado" que dirigieron los bitcoins mezclados hacia ambos intercambios.

"Este es un ejemplo claro de cómo una sola brecha de seguridad puede transformarse en una campaña de robo que se extiende durante años", afirmó Ari Redbord, director global de políticas de TRM Labs. *"Incluso cuando se utilizan mezcladores, los patrones operativos, la reutilización de infraestructura y el comportamiento en las vías de salida pueden revelar quién está realmente detrás de la actividad"*.

"Los intercambios rusos de alto riesgo continúan siendo puntos clave de salida para el

ciberdelito global. Este caso demuestra por qué la desmezcla y el análisis a nivel de ecosistema son ahora herramientas esenciales para la atribución y la aplicación de la ley”.